IN THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Please amend the following claims.

Claims 1—53 (Canceled)

54. (Currently Amended) A method for authenticating data requests, comprising:

creating a data interface for sending to a computer system, said data interface designed for promotion of a business via email, and comprising a hyperlink;

sending the data interface to an email address with intention to display the data interface on the computer system;

receiving a request for data content from a computer system, said request being provided upon ~~activation~~ following of ~~a~~ the hyperlink at the computer system and including an encrypted confirmation code that comprises a provider identification code, a computer identification code, and computer identification data, the computer identification code uniquely identifying a predetermined computer system and being dynamically generated when the ~~hyperlink~~ data interface is ~~loaded onto the predetermined computer system~~ displayed, the computer identification data including current information for identifying the computer system that ~~activated~~ followed the hyperlink, being generated when the hyperlink subsequently is ~~activated~~ followed by the computer system, and expiring in accordance with a predetermined criteria;

decrypting said encrypted confirmation code to form a decrypted confirmation code;

extracting the computer identification code, the computer identification data, and the provider identification code each from the decrypted confirmation code;

authenticating said request by comparing the computer identification code with the computer identification data;

if said request comprises a valid data request, providing the provider identification code to a valid response database system and providing the data content to the computer system; and

if said request comprises an invalid data request, identifying said request as being associated with a SPAM electronic mail message, providing the provider identification code to an invalid response database system, and presenting a dead page to the computer system, the dead page stating that the hyperlink was fraudulently generated,

wherein the hyperlink is generated by a self-aware device, incorporates said encrypted confirmation code, and is included in an electronic mail message transmitted to the computer system by a content provider system associated with the provider identification code, and

wherein said receiving the request, said decrypting said encrypted confirmation code, said extracting the computer identification code, and said authenticating said request each are performed via a processor-based system.

55. (Previously Presented) The method of claim 54, wherein said receiving said request for the data content includes receiving said request for the data content at a merchant system.

56. (Previously Presented) The method of claim 54, wherein said receiving said request for the data content includes said encrypted confirmation code being encrypted in accordance with an encryption standard selected from the group consisting of a Data Encryption Standard (DES), an Enhanced Data Encryption Standard (EDES), and an One-Way Hash Function (MD5) standard.

57. (Previously Presented) The method of claim 54, wherein said receiving said request for the data content includes receiving said data request including said encrypted confirmation code with the current computer information selected from the group consisting of at least one of an internet protocol address, a time stamp, a date stamp, and a cookie.

58. (Previously Presented) The method of claim 54, wherein said providing the data content to the computer system comprises providing the data content to the computer system to generate interest in the data content.

59. (Previously Presented) The method of claim 54, wherein said receiving said request for the data content includes said encrypted confirmation code expiring after a predetermined time interval has elapsed.

60. (Previously Presented) The method of claim 54, wherein said comparing the computer identification code with the computer identification data includes determining whether the computer identification data has expired.

61. (Previously Presented) The method of claim 54, wherein said providing the data content to the computer system includes providing advertisement content to the computer system.

62. (Previously Presented) The method of claim 54, further comprising providing the provider identification code to an accounting management system if said request comprises the valid data request.

63. (Previously Presented) The method of claim 62, wherein said providing the provider identification code to said accounting management system includes tracing an amount of remuneration owed to the content provider system.

64. (Previously Presented) The method of claim 54, further comprising denying remuneration to the content provider system if said request comprises the invalid data request.

65. (Currently Amended) A system for authenticating data requests, comprising:

a data interface generator that creates a data interface for sending to a computer system, said data interface designed for promotion of a business via email, and comprising a hyperlink;

an apparatus for sending the data interface to an email address with intention to display the data interface on the computer system;

a merchant system that receives a request for data content from a the computer system, said request being provided upon ~~activation~~ following of a the hyperlink at the computer system and including an encrypted confirmation code that comprises a provider identification code, a computer identification code, and computer identification data, the computer identification code uniquely identifying a predetermined computer system and being dynamically generated when the ~~hyperlink~~ data interface is ~~loaded onto the predetermined computer system~~ displayed, the computer identification data including current information for identifying the computer system that ~~activated~~ followed the hyperlink, being generated when the hyperlink subsequently is ~~activated~~ followed by the computer system, and expiring in accordance with a predetermined criteria;

said merchant system decrypting said encrypted confirmation code to form a decrypted confirmation code and extracting the computer identification code, the computer identification data, and the provider identification code each from the decrypted confirmation code, said merchant system authenticating said request by comparing the computer identification code with the computer identification data;

a valid response database system, said merchant system providing the provider identification code to said valid response database system and providing the data content to the computer system each if said request comprises a valid data request; and

an invalid response database system, said merchant system identifying said request as being associated with a SPAM electronic mail message, providing the provider identification code to said invalid response database system, and presenting a dead page to the computer system each if said request comprises an invalid data request, the dead page stating that the hyperlink was fraudulently generated,

wherein the hyperlink is generated by a self-aware device, incorporates said encrypted confirmation code and is included in an electronic mail message transmitted to the computer system by a content provider system associated with the provider identification code.

66. (Previously Presented) The system of claim 65, wherein said merchant system, said valid response database system, and said invalid response database system are at least partially integrated.

67. (Previously Presented) The system of claim 65, further comprising a communication system for supporting communication among said merchant system, said valid response database system, and said invalid response database system.

68. (Previously Presented) The system of claim 67, wherein said communication system supports communication with the computer system and the content provider system.

69. (Previously Presented) The system of claim 67, wherein said communication system comprises a communication link selected from the group consisting of a local area network, a wide area network, a public communication network, and the Internet.

70. (Previously Presented) The system of claim 67, wherein said communication system includes at least one wireless communication link.

71. (Previously Presented) The system of claim 65, wherein the data content comprises advertising content related to a business associated with the merchant system.

72. (Previously Presented) The system of claim 65, further comprising an accounting management system, said merchant system providing the provider identification code to said accounting management system if said request comprises the valid data request.

73. (Previously Presented) The system of claim 72, wherein said accounting management system traces an amount of remuneration owed to the content provider system.

74. (Currently Amended) A method for authenticating data requests, comprising:

creating a data interface for sending to a computer system, said data interface designed for promotion of a business via email, and comprising a hyperlink;

sending the data interface to an email address with intention to display the data interface on the computer system;

receiving a request for data content from a computer system, said request being provided upon ~~activation~~ following of ~~a~~ the hyperlink at the computer system and including an encrypted confirmation code that comprises a provider identification code, a computer identification code, and computer identification data, the computer identification code uniquely identifying a predetermined computer system and being dynamically generated when the ~~hyperlink~~ data interface is ~~loaded onto the predetermined computer system~~ displayed, the computer identification data including current information for identifying the computer system that ~~activated~~ followed the hyperlink, being generated when the hyperlink subsequently is ~~activated~~ followed by the computer system, and expiring in accordance with a predetermined criteria;

decrypting said encrypted confirmation code to form a decrypted confirmation code;

extracting the computer identification code, the computer identification data, and the provider identification code each from the decrypted confirmation code;

authenticating said request by comparing the computer identification code with the computer identification data;

if said request comprises a valid data request, providing the provider identification code to a valid response database system and providing the data content to the computer system; and

if said request comprises an invalid data request, identifying said request as being associated with a SPAM electronic mail message, and providing the provider identification code to an invalid response database system,

wherein the hyperlink is generated by a self-aware device, incorporates said encrypted confirmation code and transmitted to the computer system by a content provider system associated with the provider identification code, and

wherein said receiving the request, said decrypting said encrypted confirmation code, said extracting the computer identification code, and said authenticating said request each are performed via a processor-based system.